Mobile self-defense

Karsten Nohl <nohl@srlabs.de>
Agenda

SS7 attacks

- 3G security
- Self-defense options
SS7 network enables exchange of SMS and cryptographic keys

- Exchange SMS
- Please send new encryption key
- Please send current key
- SS7 is used between operators
- ... and network-internally

User moves into new area

Roaming user

Mobile operator

Global SS7 network

Internal SS7

MSC

MSC
Tracking over SS7 has become commonplace

Phone number ➔ Subscriber location (Cell ID)

AnytimeInterrogation

For sale: Systems that can secretly track where cellphone users go around the globe
Tracking can happen using many more signaling messages
SS7 enables mobile abuse on five frontiers

Attacker objective

A. Tracking
- Find subscriber’s whereabouts

B. Intercept
- Listen to calls, read short messages, intercept Internet traffic

C. DoS
- Interfere with user connectivity or network availability

D. Fraud
- Make illegitimate calls/send SMS; disable usage limits

E. Spam
- Send unsolicited messages

Focus of this presentation
2G + 3G transactions can be decrypted with help of SS7

1. Intercept radio transmission
2. Ask for current decryption key
SS7 enables 3G IMSI Catcher

Here is my identity (IMSI), now prove that you are the real network.

1. Prove your authenticity
2. Request key
3. Sends auth. proof

Global SS7

Mobile operator
Rerouting attacks over SS7 allow for remote intercept

<table>
<thead>
<tr>
<th>SS7 man-in-the-middle attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capture incoming calls</strong></td>
</tr>
<tr>
<td>▪ Attacker activates call forwarding over SS7 for target number</td>
</tr>
<tr>
<td>▪ When a call is received, the attacker forwards it back to the original number</td>
</tr>
<tr>
<td><strong>Capture outgoing calls</strong></td>
</tr>
<tr>
<td>▪ Attacker adds a number rewriting rule for dialed numbers</td>
</tr>
<tr>
<td>▪ Called numbers are rewritten to reach attacker and are then forwarded to intended recipient</td>
</tr>
</tbody>
</table>
Not all SS7 attacks can simply be blocked

<table>
<thead>
<tr>
<th>Abuse scenario</th>
<th>Offending SS7 message</th>
<th>Mitigation effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Local passive</td>
<td>- SendIdentification</td>
<td>Easy – Block message at network boundary</td>
</tr>
<tr>
<td>intercept</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 IMSI Catcher</td>
<td>- SendAuthenticationInfo</td>
<td>More complex – Messages are required for operations, need to be plausibility-checked</td>
</tr>
<tr>
<td>3 Rerouting attacks</td>
<td>- SS_activate/register</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- UpdateLocation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Camel messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- (Probably others)</td>
<td></td>
</tr>
</tbody>
</table>
SS7 queries

Phone number → SRI-SM → MSC, IMSI

PSI → Location (Cell ID)

PSI → TMSI

SI → Record 3G traffic → Key

SS7 queries

Radio capture

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

3G traffic

SS7 queries

Radio capture

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC, IMSI

SRI-SM

Phone number

LocaFon (Cell ID)

MSC,IMS
Agenda

- SS7 attacks
- 3G security
- Self-defense options
Remember? Intercepting GSM A5/1 calls and SMS is cheap

- A reprogrammed EUR 20 phone captures 2G calls and SMS
- Multiple such phones could be clustered for wide-scale intercept

Intercept: GSM call

Crack A5/1 key

Standard server cracks key in seconds
Intercepts 3G is also surprisingly cheap, thanks to SS7

- Software-defined radio captures 3G transactions
- We use: **BladeRF** – USD 420
- Development took 3 months

- SS7 query SendIdentification provides decryption key
- Also works for GSM A5/3
Some networks are so poorly configured that SS7 is not even needed to intercept their 3G transactions

<table>
<thead>
<tr>
<th>Network</th>
<th>Encrypts</th>
<th>Authenticates calls / SMS</th>
<th>Protects integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Flag" /></td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td><img src="image2.png" alt="Flag" /></td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td><img src="image3.png" alt="Flag" /></td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td><img src="image4.png" alt="Flag" /></td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td><img src="image5.png" alt="Flag" /></td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
</tbody>
</table>

**Risk** – Calls, SMS, and Internet traffic on these networks can be intercepted passively with a programmable radio (but without SS7)
Protection status of 3G networks is tracked in online tool

gsmmap.org network security comparison

German networks encrypt 3G, but do not all change TMSIs
Networks without USIMs are vulnerable to brute-force attacks

<table>
<thead>
<tr>
<th>NSA apparently broke 64-bit A5/3</th>
</tr>
</thead>
</table>

Encryption keys are often too short to resist NSA

<table>
<thead>
<tr>
<th>Encryption</th>
<th>SIM</th>
<th>USIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM</td>
<td>A5/3</td>
<td>64 bit</td>
</tr>
<tr>
<td></td>
<td>A5/4</td>
<td>64 bit</td>
</tr>
<tr>
<td>UMTS</td>
<td>UEA/1 or 2</td>
<td>64 bit</td>
</tr>
</tbody>
</table>

Source – The intercept: wolframite-encryption-attack.pdf
Agenda

- SS7 attacks
- 3G security

Self-defense options
Many mobile network abuse scenarios can be detected

<table>
<thead>
<tr>
<th>Attack scenario</th>
<th>Detection heuristic</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Attacks</td>
<td></td>
</tr>
<tr>
<td>• SIM OTA attacks</td>
<td>• Unsolicited binary SMS</td>
</tr>
<tr>
<td>• Semi-lawful Tracking through silent SMS</td>
<td>• Silent SMS</td>
</tr>
<tr>
<td>• SS7 abuse: Tracking, Intercept, etc.</td>
<td>• Empty paging</td>
</tr>
<tr>
<td>SS7 Attacks</td>
<td></td>
</tr>
<tr>
<td>• Tracking or Intercept through 2G or 3G fake base station</td>
<td>• Unusual cell configuration and cell behavior (detailed</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>IMSI Catcher</td>
<td>later in this chapter)</td>
</tr>
<tr>
<td>• Insufficient encryption leads to Intercept and Impersonation</td>
<td></td>
</tr>
<tr>
<td>• Lack of TMSI updates enables Tracking</td>
<td></td>
</tr>
<tr>
<td>Network Security</td>
<td></td>
</tr>
<tr>
<td>• Encryption level and key change frequency</td>
<td></td>
</tr>
<tr>
<td>• TMSI update frequency</td>
<td></td>
</tr>
</tbody>
</table>
New tool detects common abuse scenarios

<table>
<thead>
<tr>
<th>Tool name</th>
<th>SnoopSnitch</th>
</tr>
</thead>
</table>
| **Purpose** | - Collect network traces on Android phone and analyze for abuse  
- Optionally, upload to GSMmap for further analysis |
| **Requirements** | - Android 4.1 or newer  
- Rooted, (CyanogenMod may work)  
- Qualcomm chipset: Samsung S5/ S4/S3 Neo, Sony Z1, LG G2, Moto E, and many more |
| **Source**  | Google Play: Search for *SnoopSnitch* |

<table>
<thead>
<tr>
<th><strong>Tool</strong></th>
<th><strong>SMS &amp; SS7 attacks</strong></th>
<th><strong>IMSI Catcher</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last analysis</strong></td>
<td>Dec 22, 2014 4:35:09 PM</td>
<td></td>
</tr>
<tr>
<td><strong>Tool</strong></td>
<td><strong>Network Security</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Sending SMS to invalid destination</strong></td>
<td>Stop Test</td>
<td></td>
</tr>
<tr>
<td><strong>Provider results in comparison</strong></td>
<td><strong>Intercept</strong></td>
<td><strong>Impersonation</strong></td>
</tr>
<tr>
<td>Your test result</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Your network T-Mobile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vodafone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-Plus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3G</td>
<td>2G</td>
<td>2G</td>
</tr>
<tr>
<td>higher protection</td>
<td></td>
<td>lower protection</td>
</tr>
</tbody>
</table>
IMSI catcher detection analyzes a cell’s configuration and behavior

SnoopSnitch combines a number of IMSI Catcher heuristics

Suspicious cell **configuration**
- Encryption downgrade / no encryption
- High cell reselect offset
- Large number of paging groups
- Low registration timer

Suspicious cell **behavior**
- Delayed *Cipher Mode Complete* acknowledgement
- *Cipher Mode Complete* message without IMEISV
- ID requests during location update
- Paging without transaction
- Orphaned traffic channel

A number of other rules could not be implemented based on data available from Qualcomm chipsets. (Future work?)
SnoopSnitch collects data in the background and on request.

Directed attacks are constantly analyzed in a background process.

Network tests are uploaded only on demand.

Alerts can be shared for further analysis.
It’s now on you to contribute data and progress the toolbox of self-defense apps

**Mobile self-defense strategy**

1. Check your network operator on [gsmmap.org](http://gsmmap.org) for vulnerabilities; possibly switch to a more secure operator

2. Install **SnoopSnitch** from Google Play (needs Android 4.1+, Qualcomm chipset, root, may not work with custom ROM)

3. Conduct a network test and upload any attack alarms (SMS, SS7, IMSI catcher) for further analysis

4. Contribute to the SnoopSnitch code or use the source to build your own application based on raw 2G/3G/4G data
Thank you!

Many thanks to Alex Senier, Luca Melette, Lukas Kuzmiak, Linus Neumann, Jakob Lell, and dexter!

Research supported by OPEN TECHNOLOGY FUND

Questions?

Karsten Nohl <nohl@srlabs.de>